Amendments to the Specification:

Please replace the paragraph beginning on page 2, line 21, with the following amended paragraph:

The previous depictions for implementation of HEC-based cryptosystems were mainly ~~focussed~~ focused on the efficiency of implementation and neglected the resistance of implementation to attacks by means of differential power analysis.

Please delete the paragraph beginning on page 2, line 29.

Please replace the paragraph beginning on page 4, line 1, with the following amended paragraph:

As already described above, there are various ways of structuring and refining the teaching of the present invention advantageously. ~~For this reference is made to the claims following from claim 1.~~

Please replace the paragraph beginning on page 9, line 18, with the following amended paragraph:

To summarise it can be found that curve randomization in uneven characteristic is an effective and efficient protective measure against attacks based on the method of differential power analysis. The total count of the necessary field operations in K is 11g+1. ~~To summarise it can be found that curve randomization in uneven characteristic is an effective and efficient protective measure against attacks based on the method of differential power analysis. The total count of the necessary field operations in K is 11g+1.~~

Please replace the paragraph beginning on page 10, line 1, with the following amended paragraph:

The arguments presented above with regard to the general isomorphisms of curves also apply unchanged for the case discussed below, where K is a field of even characteristic. In this case however $h(x)\tilde{h}(x)$ must ~~no~~ not equal zero; in other words this means that the use of general isomorphisms is less efficient than in the case of uneven characteristic.

Please replace the paragraph beginning on page 13, line 4, with the following amended paragraph:

To summarise, for the method described above of curve randomisation it can be found that this counter-measure for hyperelliptic curves of genus 2 in even characteristic

- either is not adequate because ~~two~~ too few co-efficients can be randomized,
- or inhibits the power of the cryptographic system as the counter-measure uses the general isomorphisms according to equation (4) and leaves the co-efficients of h lying outside (4) F^2.